IN THE SPECIFICATION

Please replace the paragraph at page 1, lines 20-29, with the following rewritten paragraph:

Various kinds of software data (hereinafter referred to as content) such as audio data including music, image data including movies, game programs and various application programs, are provided to a user as stored on an information recording medium including, e.g., a DVD (Digital Versatile Disc), an MD (Mini Disc) (registered Trademark), a CD (Compact Disc), or a high-density recordable disc using blue laser (Blu-ray Disc) (registered Trademark). The user can play back content for use in a user device including a PC (Personal Computer), a disc player, i.e., in a playback apparatus.

Please replace the paragraph at page 21, lines 12-24, with the following rewritten paragraph:

As shown in Fig. 3, a message for processing, i.e., the version number 151 and the revoked disc ID list 152 shown in Fig. 2 in this case, is divided into 8-byte blocks (the divided messages are hereinafter referred to as M1, M2, ···, MN). First, an Initial Value (hereinafter referred to as IV) is XORed with M1 (the result is I1). Next, I1 is inputted to a DES (Data Encrypting Standard) encrypting section using a key (hereinafter referred to as K1) (its output is E1). Successively, E1 is XORed with M2, and its output I2 is inputted to the DES encrypting section using the key K1 (an output E2). Thereafter, this processing is repeated to encrypt all the messages. The last output EN is the Message Authentication Code (MAC).

Please replace the paragraph at page 23, line 29 to page 24, line 1, with the following rewritten paragraph:

As is apparent from Fig. 4, the ~~three~~ four devices 0, 1, 2, 3 included in one group hold shared keys K00, K0, KR as the device keys (DNKs: Device Node Keys) stored on their devices.

Please replace the paragraph at page 29, lines 15-23, with the following rewritten paragraph:

For example, service providing situation data shown in ~~Fig. 8 (a)~~ Fig. 8 is service providing situation data as to:

title identification information: aaaa; and

title-unique value: bbbb,

and is a recording of how many times a Service 1 and a Service 2 associated with content corresponding to this title have so far been provided in response to service providing requests based on discs having a disc ID 1 and a disc ID 2, respectively.

Please replace the paragraph at page 39, lines 12-17, with the following rewritten paragraph:

In step S201, the controller 408 of the information recording apparatus (user device) 400 extracts signature data ~~SIG(w)~~ Sig (w) in disc ID (w). Note that the disc ID is denoted a disc ID(w) since it takes a value specific to each of individual discs (w) where w = 1, 2, ··· W, given the number of discs to be manufactured being W.

Please replace the paragraph at page 39, lines 19-25, with the following rewritten paragraph:

In step S202, the controller 408 generates M(w)' from the signature data ~~SIG(w)~~ Sig(w) read in step S201, on the basis of a public key and published parameters of the management apparatus [[12]] 201 (Central Authority CA). The message is also denoted similarly to the disc ID(w). A message M(w) indicates that the message is made to correspond to each of the discs.

Please replace the paragraph at page 40, lines 15-22, with the following rewritten paragraph:

This Setting Example 2 is different from the Setting Example 1 only in the title-unique value S in place of M. Thus, its disc ID verifying processing sequence in the information processing apparatus (user device) 400 is similar to that in the Setting Example 1, except that data generated from the signature data in step S202 is a message ~~S'(w)~~ S(w)' and that data for comparison in step S203 is data S(w) contained in the disc ID.

Please replace the paragraph at page 41, lines 8-12, with the following rewritten paragraph:

In step S302, the controller 408 judges whether or not the data p(w) extracted in step ~~S302~~ S301 is a prime. The controller 408, when having judged that the data p(w) is a prime, proceeds to step S303; otherwise, it proceeds to step S304.

Please replace the paragraph at page 43, lines 11-21, with the following rewritten paragraph:

In step S405, the controller 408 stops (prohibits) decryption and playback of the encrypted content recorded in the information recording medium ~~200c~~ 200. In step S406, the controller 408 transmits the disc ID read in step S401 to the service providing server, and further, in step S407, receives a service from the service providing server. Note that the service providing server verifies the disc ID received from the information processing apparatus (user device) 400 in step S406, and then executes the service providing processing only in a case where the disk ID has been validated.

Please replace the paragraph at page 52, lines 2-8, with the following rewritten paragraph:

Furthermore, the disc ID has been described as differing from one disc to another ~~in the above-mentioned embodiment~~. However, the disc ID may be common to a unit of, e.g., 10 discs, 100 discs, or 1,000 discs, and the service providing limit set for a single disc ID may be determined in consideration of the number of discs in a group.